UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/620,817	07/16/2003	Stephen F. Bisbee	003670-104	1237

7590   05/13/2008

Burns, Doane, Swecker & Mathis, L.L.P.
P.O. Box 1404
Alexandria, VA 22313-1404

EXAMINER
DAVIS, ZACHARY A

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
05/13/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _31 December 2007_.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-35_ is/are pending in the application.
    4a) Of the above claim(s) _19-33_ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) _1-18,34 and 35_ is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on _16 July 2003_ is/are: a)☐ accepted or b)☒ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All   b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application
6)☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1.   Applicant's election of Group I, Claims 1-18, 34, and 35, in the reply filed on 03

August 2007 is acknowledged. Because applicant did not distinctly and specifically

point out the supposed errors in the restriction requirement, the election has been

treated as an election without traverse (MPEP § 818.03(a)). Specifically, Applicant

merely alleges that "the inventions of Groups I and II should properly be examined

together" and "Groups I and II appear to be capable of being examined together without

a serious burden" (page 2 of the response received 03 August 2007). However, the

Examiner notes that Applicant has not cited any evidence in support of these

assertions, nor has Applicant addressed the showings in the requirement for restriction

(mailed 11 June 2007) that the inventions are independent or distinct and are classified

separately. Further, although Applicant notes that "claim 19 refers to claim 1" (page 2 of

the response received 03 August 2007), this was previously addressed in the

requirement for restriction, which noted that Claim 19 did not require any of the specifics

of Claim 1, but merely referred to the retrieved status from a certificate status service as

in Claim 1 (see page 3 of the requirement mailed 11 June 2007). Therefore, Applicant's

arguments amount to a general allegation that does not distinctly and specifically point

out the supposed errors in the requirement for restriction, which fails to comply with the

requirements of 37 CFR 1.111(b).

2.   Claims 19-33 are withdrawn from further consideration pursuant to 37 CFR

1.142(b) as being drawn to a nonelected invention, there being no allowable generic or

linking claim. Election was made **without** traverse in the reply filed on 03 August 2007.

Response to Amendment

3.   Applicant is thanked for their detailed response to the supplemental requirement

for information under 37 CFR 1.105 set forth 02 November 2007. It is duly noted that

Claims 1-18, 34, and 35 are only considered to claim priority under 35 U.S.C. 119(e) to

Provisional Application Serial No. 60/397,178, with the exceptions noted by Applicant in

the response received 31 December 2007, and that none of the elected claims are

entitled to a claim of priority to any of the other noted parent applications under 35

U.S.C. 119 or 120.

Response to Arguments

4.   Applicant's arguments filed 30 March 2007 have been fully considered but they

are not persuasive.

        Claims 1-15 were rejected under 35 U.S.C. 102(e) as anticipated by Koehler, US

Patent 6301658. Claims 16-18 were rejected under 35 U.S.C. 103(a) as unpatentable

over Koehler in view of Konheim, US Patent 4264782.

Generally in response to the previous Office action, Applicant asserts that the

Examiner "extends the disclosure of the Koehler patent in ways that were not intended,

not known to one skilled in the art at the time, and that deviate from the Internet PKI

standards in use at the time" (page 19 of the present response). However, the

Examiner respectfully disagrees, noting that the language of the claims has been given

its broadest reasonable interpretation, and the disclosures within Koehler are seen to be

encompassed by that broad interpretation of the claims. Applicant's arguments largely

present a much narrower view of the claims than of everything that is encompassed by

the broad language of the claims (see pages 19-21 of the present response, for

example). For example, Applicant asserts that their "CSS goes well beyond the Koehler

patent disclosure by addressing the methods to work concurrently with or reject any CA

or PKI, not dependent on what policies, practices, procedures, and certificate status

reporting means are employed" (page 21 of the present response). However, the

claims are not this narrow; the broad language of the claims encompasses the invention

as defined in the specification but also, for example, the certificate status caching

method of Koehler. In response to applicant's argument that the references fail to show

certain features of applicant's invention, it is noted that the features upon which

applicant relies are not explicitly recited in the rejected claims. Although the claims are

interpreted in light of the specification, limitations from the specification are not read into

the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Applicant's arguments regarding Claims 3, 4, 10, and 15, for example (see pages

21-22 of the present response), do not comply with 37 CFR 1.111(c) because they do

not clearly point out the patentable novelty which he or she thinks the claims present in

view of the state of the art disclosed by the references cited or the objections made.

The arguments merely assert what is "broadly encompassed" by those claims but do

not point out any alleged differences from the prior art.

In reference to independent Claim 1, Applicant argues that Koehler does not

disclose providing identifying information from the CA that issued the certificate (pages

22-23 of the present response). In particular, Applicant argues that only CRL based

certificate status reporting was supported and that the "identifying information disclosed

in Applicants' Claim 1 are [sic] the set of protocols and parameters necessary to retrieve

certificate status from an approved set of diverse issuing CAs and certificate status

responders" (page 23 of the present response). However, the information identified in

the claim does not necessarily require the specifics that Applicant ascribes to the

claimed information; the claim merely requires that the information is "needed for

retrieving a status of an authentication certificate from an issuing CA", not that specific

protocols be supported (see Claim 1; compare to Applicant's assertion on page 23 of

the present response that the information support CRLs, OCSP, LDAP, etc). In

response to applicant's argument that the references fail to show certain features of

applicant's invention, it is noted that the features upon which applicant relies (i.e.,

various certificate status protocols; also that the information "must be supplied to the

CSS separately"; see page 23 of the present response) are not recited in the rejected

claim(s). Although the claims are interpreted in light of the specification, limitations from

the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26

USPQ2d 1057 (Fed. Cir. 1993). Similarly, although Applicant asserts that it would not be obvious to modify the Koehler disclosure "to work with multiple CRL based CA hierarchies" etc., and that "new CA registration, communication means, certificate status protocols, and cache management capabilities" would have to be added to Koehler (see page 24 of the present response), these various issues are also not recited in independent Claim 1.

Applicant further disagrees that the server in Koehler acts as a connector and asserts that Koehler "cannot retrieve non-CRL based certificate status from multiple different independent CAs and CA hierarchies or where different trust policies are employed" (pages 24-25 of the present response). Applicant further disagrees that communication occurs when authentication is performed and asserts that the connector enables the CSS to "retrieve all forms of certificate status reporting from any CA, PKI or certificate status responder, regardless of whether they are dependent, independent or use different security or communications technologies or protocols" (page 25 of the present response). However, again, the Examiner notes that the features upon which Applicant relies are not recited in rejected Claim 1, and although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. Similarly, Applicant traverses the conclusion that Koehler determines the status of the certificate, asserting that the verification server caches a certificate's status and Koehler does not disclose any means other than CRLs (pages 25-26 of the present response).

The Examiner respectfully disagrees with Applicant's above arguments, noting

that the terms in the claims have been given their broadest reasonable interpretation.

For example, regarding the connector, Claim 1 merely requires that the connector be

configured and communication be performed according to that connector; likewise, as

previously set forth, the server in Koehler is configured to connect to the CA and

communicates according to that connector (see Figure 1, where the server connects

that cache to the repository; see also column 5, line 42-column 7, line 64 in general).

Further, Koehler clearly discloses retrieving the status of the authentication certificate as

claimed (see again, column 5, line 42-column 7, line 64 in general, where certificates

are verified and CRLs are checked for a certificate's status as to whether it has been

revoked).

In reference to independent Claim 11, Applicant argues that Koehler does not

suggest the CSS being used by a trusted third party repository of information objects for

obtaining certificate status (see page 26 of the present response). First, the Examiner

notes that Applicants have admitted as prior art that, in general, it is well known for a

third party repository to obtain certificate status (see page 1, lines 22-28 of the present

specification). Further, Applicant disagrees that the certificate repository of Koehler is

not a repository of information objects because Koehler does not describe "dealing with

any **other** information object **other** than the certificates" and "does not suggest any

other form of information object" (pages 26-27 of the present response, emphasis

added). The Examiner notes that, by use of the term "other", Applicant has admitted

that the certificates are, in fact, information objects and the repository thus must contain

information objects. Additionally, Applicant asserts that the Koehler patent would not have suggested methods that "insure that one and only one authoritative copy ever exist [sic], and that this authoritative copy is always held and never released by the trusted third-party repository" and that digital signatures are validated by the trusted third party repository (page 27 of the present response). However, again, the Examiner notes that the features upon which Applicant relies are not recited in rejected Claim 11, and although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. Again, see *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In reference to independent Claim 15, Applicant argues that Koehler uses a timestamp to indicate whether a CRL is newer than a previously validated certificate, and that the claimed invention uses the time-to-live etc. to determine when status needs to be updated (pages 27-28 of the present response). The Examiner fails to appreciate this argument, since Koehler uses timestamps and other time data to determine whether a new CRL needs to be accessed, i.e. status needs to be updated (see column 7, lines 11-59); this does not differ from Applicant's stated use of the time-to-live. Applicant further argues that the claims "use a real-time certificate status protocols [sic]"; however, once again, the Examiner notes that the features upon which Applicant relies are not recited in rejected Claim 15 (e.g., "real-time" does not appear in the claims whatsoever), and although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. Again, see *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

Drawings

5.   The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: 114 (page 19, line 16); 301, 303 (page 21, line 30); 305, 307 (page 22, line 8); 309 (page 21, line 31). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application.

6.   The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 159 (see Figure 1); 809, 815 (see Figure 8). Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application.

7.   Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be

notified and informed of any required corrective action in the next Office action. The

objection to the drawings will not be held in abeyance.

Specification

8.   The disclosure is objected to because of the following informalities:

The specification contains minor typographical and other errors. For example, on

page 1, lines 22-24, in the phrase "advantageously uses Applicants' Trusted Custodial

Utility that holds electronic original records and comparable system roles as a virtual

electronic vault", it is not clear what the phrase "and comparable system roles" is

intended to modify or coordinate with. In the sentence at page 2, lines 19-25, it is not

clear what the subject of "has generated" in line 23 is intended to be. In the sentence at

page 12, line 32-page 13, line 1, the phrases "the means of communication" and "of

processing certificate status for every CA" do not appear to be in parallel construction.

On page 14, line 27, it appears that, in the phrase "to the form a signature block", "the"

should be deleted. On page 14, line 30, the parenthetical notation "(integrity)" is

generally unclear. On page 15, line 4, it appears that "Conversely" may be intended to

read "Alternatively" or "Alternately" or similar. On page 17, line 4, it appears that "in"

should be inserted after "result". On page 18, lines 6-8, it is not clear what the phrase

"and not to exceed the interval established in the TCU security policy" is intended to

modify or coordinate with. On page 18, lines 15-16, it appears that, in the phrase

"objects are be uploaded", "are be" is intended to read either "are to be" or simply "are".

On page 21, line 23, it is not clear what the phrase "or directory" is intended to coordinate with. On page 27, line 26, it appears that "Electronic Original", while capitalized, may be intended to refer to a trademark and, if so, should be designated as such. On page 29, lines 4-12, the phrase "consists of inclusion..." at lines 6-7 is not in parallel construction and/or does not appear to have a clear subject. On page 29, lines 30-31, in the phrase "local data and time is protected", "is" is intended to read "are". Similarly, on page 29, line 31-page 30, line 2, it appears that "it is accurate" is intended to read "they are accurate"; "it falls" is intended to read "they fall"; and in the phrase "the local date and time is not before and not after", "is" is intended to read "are". On page 30, lines 4-5, in the phrase "a violation of authentication certificate validity period", it appears that an article (e.g. "an" or "the") should be inserted before "authentication". On page 30, line 22, it appears that "signatures blocks" is intended to read either "signature blocks" or simply "signatures". On page 30, line 30, it appears that "falls" is intended to read "fall". On page 31, line 17, in the phrase "returns status", it appears that "the" should be inserted after "returns". On page 31, lines 17-18, in the phrase "If certificate status is not present or outside the time-to-live interval", it appears that "the" or "any" should be inserted before "certificate", and "is" should be inserted before "outside". On page 31, line 20, it appears that "the" should be inserted before "certificate status reporting component". On page 31, line 22, it appears that "the" should be inserted before "CSS configuration store". On page 31, line 23, it appears that "the" should be inserted before "session" and also between "with" and "component". On page 32, line

29, it appears that "certificate are issued" should read either "certificates are issued" or

"a certificate is issued".

Further, it is noted that Applicant does not clearly appear to consistently

distinguish between the phrase "electronic original" and Applicant's trademarked phrase

"Electronic Original" throughout the present application.

Appropriate correction is required. The above is not to be considered an

exhaustive list of errors in the specification. The lengthy specification has not been

checked to the extent necessary to determine the presence of all possible minor errors.

Applicant's cooperation is requested in correcting any errors of which applicant may

become aware in the specification.

9.   The specification is objected to as failing to provide proper antecedent basis for

the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction

of the following is required: There is not proper antecedent basis for all of the subject

matter of new Claims 34 and 35. Although Applicant asserts that there is support for

Claim 34 at page 18, lines 9-24; page 31, lines 13-25, and page 34, lines 3-27 of the

present specification (see page 18 of the response received 30 March 2007), the

Examiner notes that none of these cited portions disclose a "background low priority

garbage collection utility". Further, although Applicant asserts that there is support for

Claim 35 at page 35, lines 3-10 of the present specification (see page 18 of the

response received 30 March 2007), the Examiner notes that this cited portion does not

disclose specifically designating any CSS as secondary. See below regarding the

rejection under 35 U.S.C. 112, first paragraph, for further detail.

Claim Objections

10.   Claim 2, 5, and 18 are objected to because of the following informalities:

Claim 2 uses the pronoun "they". Care should be taken when using pronouns to

ensure that their antecedent is clear.

In Claim 5, in lines 4-5, it appears that commas should be inserted between "or"

and "if" and between "exceeded" and "clearing". Further, it appears that "the" should be

inserted before "certificate status reporting component" in line 10.

Claim 18 uses the pronoun "it". Care should be taken when using pronouns to

ensure that their antecedent is clear.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

11.   The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of
> making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the
> art to which it pertains, or with which it is most nearly connected, to make and use the same and shall
> set forth the best mode contemplated by the inventor of carrying out his invention.

12.   Claims 34 and 35 are rejected under 35 U.S.C. 112, first paragraph, as failing to

comply with the written description requirement. The claim(s) contains subject matter

which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Specifically, there is not sufficient written description for the subject matter of the limitation in Claim 34 of "a background low priority garbage collection utility". Although Applicant asserts that there is support for Claim 34 at page 18, lines 9-24; page 31, lines 13-25, and page 34, lines 3-27 of the present specification (see page 18 of the response received 30 March 2007), the Examiner notes that none of these cited portions disclose or even mention a "background low priority garbage collection utility", and the phrase does not appear anywhere else in the specification.

Additionally, there is not sufficient written description for the subject matter of the limitation in Claim 35, namely that any particular CSS is explicitly "designated secondary". Although Applicant asserts that there is support for Claim 35 at page 35, lines 3-10 of the present specification (see page 18 of the response received 30 March 2007), the Examiner notes that this cited portion does not disclose specifically designating any CSS as secondary, although it does disclose querying other CSSes rather than a CA itself.

13.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

14.   Claims 5, 9, 11-18, and 34 are rejected under 35 U.S.C. 112, second paragraph,

as being indefinite for failing to particularly point out and distinctly claim the subject

matter which applicant regards as the invention.

Claim 5 recites "the time-to-live or use-counter threshold" in lines 4-5. There is

insufficient antecedent basis for this limitation in the claims.

Claim 9 recites the limitation "a connector embeds more than one certificate

status check in a single communicating step". However, this is generally unclear, as

"connector" does not necessarily appear to encompass a device that could perform the

action of "embedding"; further, it is not clear how anything could be "embedded" within a

nebulous concept such as a "step".

Claim 11 recites steps beginning "if the status type is Certificate Revocation List"

(lines 10-12) and "if the status type is not CRL" (lines 13-14). However, it is not clear

whether the steps following the step "if the status type is not CRL" (see lines 15-24) are

intended to be performed always or are only intended to if the status type is not CRL.

Therefore, it is not clear exactly which steps are to be performed when.

Claim 15 recites "A Certificate Status Service" in the preamble, which would

appear to be a device, apparatus, article of manufacture, or perhaps a software

program running on one of the above (see, for example, Figure 8, where the CSS is

clearly a computer). However, the body of the claim recites various steps to be

performed, as though the claim were directed to a method. Therefore, it is not clear

whether the claim is intended to be directed to a device or to a method, which renders

the claim indefinite. Further, the claim recites a step that is performed "when the

certificate's issuing CA uses CRLs for indicating status" (lines 4-6) and another step to

be performed "otherwise" (lines 7-8). However, it is not clear whether the steps

following the step performed "otherwise" (see lines 9-15) are intended to be performed

always or are only intended to be performed if the issuing CA does not use CRLs.

Therefore, it is not clear exactly which steps are to be performed when.

Claim 18 recites "searches the cache memory for a status where the time-to-live

data element exceeds the current local time or a last-accessed data element indicating

an oldest date". However, the two items "a status" and "a last-accessed data element"

do not appear to be clear parallels, which renders the claim unclear.

Claims not specifically referred to above are rejected due to their dependence on

a rejected base claim.

Claim Rejections - 35 USC § 102

15.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

16.   Claims 1-15 are rejected under 35 U.S.C. 102(e) as being anticipated by

Koehler, US Patent 6301658.

In reference to Claim 1, Koehler discloses a method of providing a Certificate Status Service ("CSS") for checking validities of authentication certificates issued by respective issuing Certification Authorities ("CAs") that includes identifying information needed for retrieving a status of an authentication certificate from an issuing CA (column 5, lines 14-20); configuring a connector based on the identified information for communicating with the issuing CA and communicating with the issuing CA according to the configured connector when the status of the authentication certificate is queried (column 5, lines 46-55); and retrieving the status of the authentication certificate (column 5, lines 53-55; column 6, lines 1-3); wherein the issuing CA and the connector are designated on a list of approved CAs in a configuration store (column 6, lines 3-8).

In reference to Claim 2, Koehler further discloses that a local date and time are checked for whether they fall within a validity period indicated in the authentication certificate, and an invalid status is reported if the local date and time fall outside the validity period (column 5, line 65-column 6, line 3).

In reference to Claim 5, Koehler further discloses checking a local cache memory for status, and if the status is found in the local cache memory and the local date and time are within the validity period, retrieving the status from the local cache memory; and if the status is not found in the local cache memory, the CSS establishes a communication session with a certificate status reporting component of the issuing CA, composes a certificate status request according to the configured connector, retrieves the status from the certificate status reporting component, closes the communication session with certificate status reporting component, and adds at least the authentication

certificate's identification, status, and time-to-live to the local cache memory (column 5,

line 65-column 6, line 27).

In reference to Claim 3, Koehler further discloses that the issuing CA is included

in the list of approved CAs by vetting and approving the issuing CA according to

predetermined business rules, and if the issuing CA is vetted and not approved, the

issuing CA is designated on a list of not-approved CAs in the configuration store

(column 5, lines 21-36; column 8, lines 16-21).

In reference to Claim 4, Koehler further discloses that vetting and approving the

issuing CA includes registering a representation of the CA's trusted authentication

certificate with the CSS and adding at least the representation, status and a time-to-live

data element to a local cache memory, and that a connector is configured for retrieving

the added status when the status of the trusted authentication certificate is queried

(column 7, lines 12-16; column 8, lines 21-36).

In reference to Claim 6, Koehler further discloses that when the certificate status

is indicated by a Certificate Revocation List (CRL), according to a publication schedule

of the issuing CA, the CSS retrieves the CRL from a certificate status reporting

component listed in the configuration store, the CSS clears a cache memory associated

with the issuing CA, and the CSS determines the status of the authentication certificate

from the CRL and stores the status in the cache memory associated with the issuing CA

(column 5, line 65-column 6, line 27).

In reference to Claim 7, Koehler further discloses that when the certificate status

is indicated by a Delta Certificate Revocation List ("ΔCRL"); upon notification by the

issuing CA that a ΔCRL is available, the CSS retrieves the ΔCRL from a certificate

status reporting component listed in the configuration store; if the ΔCRL is a complete

CRL, then the CSS clears a cache memory associated with the issuing CA, determines

the status from the CRL, and stores the status in the cache memory; and if the ΔCRL

contains only changes occurring after publication of a full CRL, the CSS determines the

status from the ΔCRL, and stores the status in the cache memory (column 7, lines 12-

34).

In reference to Claim 8, Koehler further discloses communicating according to a

sequence of connectors (column 5, lines 42-46; column 8, lines 37-45).

In reference to Claim 9, Koehler further discloses more than one certificate status

checks in a single communicating step (column 5, lines 42- 46; column 8, lines 37-45).

In reference to Claim 10, Koehler further discloses that the authentication

certificate is not used for identification (column 5, lines 42-46; column 8, lines 37-45).

In reference to Claim 11, Koehler discloses a method of retrieving a status of an

authentication certificate issued by an issuing Certification Authority ("CA") in response

to a query from a trusted third-party repository of information objects to a Certificate

Status Service ("CSS") to validate the authentication certificate's status that includes

locating and reporting the status if the status is present and current in a cache

memory of the CSS (column 5, line 63-column 6, line 8); otherwise performing the steps

of: obtaining a status type and retrieval method from a CSS configuration store (column

5, line 63-column 6, line 8); if the status type is Certificate Revocation List ("CRL") and

the last retrieved CRL is current, but the status is not found in the cache memory, then

reporting the status as valid (column 6, lines 9-27); if the status type is not CRL, then

composing a certificate status request according to the status type (column 6, lines 9-27

- if no entry, status composed from repository); establishing a communication session

with the issuing CA (column 5, lines 48-55; column 6, lines 28-41); retrieving the status

from a status reporting component of the issuing CA using the obtained retrieval method

and ending the communication session (column 6, lines 56- 66); interpreting the

retrieved status (column 6, lines 56-66); associating, with the interpreted retrieved

status, a time-to-live value representing a period specified by a CSS policy for the status

type (column 6, lines 56-66); adding at least the authentication certificate's identification,

status, and time-to- live values to the cache memory (column 5, line 63-column 6, line

8); and reporting the status to the trusted third-party repository of information objects in

response to the query (column 8, lines 2-21).

In reference to Claim 12, Koehler further discloses that the CSS uses a certificate

status protocol in the communication session (column 5, lines 44-48).

In reference to Claim 13, Koehler further discloses that more than one status is

retrieved using the obtained retrieval method (column 5, lines 42-48).

In reference to Claim 14, Koehler further discloses that the authentication

certificate is not used for identification (column 5, lines 42-46; column 8, lines 37-45).

In reference to Claim 15, Koehler discloses a Certificate Status Service ("CSS")

for providing accurate and timely status indications of authentication certificates issued

by issuing Certification Authorities ("CAs") that includes providing a status of an

authentication certificate as indicated by a Certificate Revocation List ("CRL") when the

certificate's issuing CA uses CRLs for indicating status (column 7, lines 12-34);

otherwise, providing the status indicated by a cache memory when the cache memory

includes a status and a time-to-live data element is not exceeded (column 7, lines 17-

19); if the time-to-live data element is exceeded, clearing the status from the cache

memory (column 5, lines 47-49); requesting and retrieving the status using a real-time

certificate status reporting protocol when the status is not in the cache memory (column

5, lines 53-55); adding at least the certificate's identification, status, and time-to-live data

element to the cache memory (column 5, line 63-column 6, line 8); and providing the

retrieved status (column 5, line 63-column 6, line 8).

Claim Rejections - 35 USC § 103

17.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

18.   Claims 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Koehler in view of Konheim, US Patent 4264782.

        In reference to Claim 16, Koehler discloses everything as described above with

reference to Claim 15; however, Koehler does not explicitly disclose a status use-

counter data element. Konheim discloses a status use-counter data element that is

added to the cache memory; is incremented or decremented every time the certificate's

status is checked; and if the status use-counter data element passes a threshold, then

the status is provided and .the cache memory is cleared with respect to the status

(column 11, lines 58-68; column 12, lines 37-47). Therefore, it would have been

obvious to one of ordinary skill in the art at the time the invention was made to combine

Koehler's digital certificate authentication system with Konheim's identity verification

method utilizing a use-counter to check memory access in order to protect against the

re-use of a previously verified transaction (Konheim, column 7, lines 4-6).

In reference to Claim 17, Koehler and Konheim further disclose that a status last-

accessed data element is added to the cache memory, and the status last-accessed

data element in conjunction with the status use-counter data element enable

determination of an activity level of the certificate's status (Koehler, column 6, lines 17-

22).

In reference to Claim 18, Koehler and Konheim further disclose that when a

request is made to the CSS to retrieve a status of a new certificate and the cache

memory has reached an allocated buffer size limit, the CSS searches the cache

memory for a least-accessed data element indicating an oldest date and clears the

respective cache memory entry; and the CSS then retrieves the requested status,

places it in the cache memory, and provides the requested status (Koehler, column 6,

lines 12-27; column 7, lines 52-57, where the timestamp is updated, which thus clears

the memory and enters a new value).

Conclusion

19.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

  a. Datar et al, US Patent 6351812, discloses a method in which certificate

status information is cached.

  b. Dierks, US Patent 6948061, discloses a method for secure transactions in

which certificate status can be cached.

  c. Hope et al, US Patent 7120793, discloses a system that includes a

responder that determines whether a certificate has been revoked.

  d. Claxton et al, US Patent 7177839, discloses an electronic transaction

system that includes a Certificate Status Service.

  e. Micali, US Patent 7337315, discloses a system for efficient certificate

revocation.

  f. Delaney et al, US Patent 7349912, discloses a system in which a server

stores real time retrieved certificate status.

  g. Kivinen et al, US Patent 7356693, discloses a method for producing CRLs

that includes root CRLs and online certificate status.

  h. Dulin et al, US Patent Application Publication 2002/0029200, discloses a

system for providing certificate validation that includes a certificate status check

service.

       i.   Fraser et al, US Patent Application Publication 2003/0130960, discloses a

bridging service providing interoperability between, for example, CRLs and

OCSP.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Zachary A. Davis whose telephone number is (571)272-

3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate

Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone

number for the organization where this application or proceeding is assigned is 571-

273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ZAD/
Examiner, Art Unit 2137

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137